UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,952	12/11/2000	Aravind Sitaraman	CISCO-3294	4939

7590 07/11/2005

David B. Ritchie
Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640

EXAMINER	
PATEL, ASHOKKUMAR B	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 07/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/734,952	SITARAMAN ET AL.	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) *1, 10-12, 21-23, 32-35, 44 and 45* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 are subject to examination. Claims 1, 10-12, 21-23, 32-35, 44 and 45 have been cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/05/2005 has been entered.

Response to Arguments

3. Applicant's arguments filed 05/05/2005 have been fully considered but they are not persuasive for the following reasons:

The 35 U.S.C. § 102 & 103 Rejections:

Applicant's argument:

"By contrast, in the DOS attack as addressed by the present claims and not by Lin, the attacker is a "connected" "subscriber" who uses a sufficient t number of GETS or POSTS to bog the target TCP down by sheer volume of traffic. The claims go beyond the issue of establishing a connection. The subscriber has been authorized to make a connection and the connection has been made. What the connected subscriber has not yet been "authorized" to do is exceed the "maximum HTTP request frequency." Rather than establish one and only one maximum frequency, the claims allow each connected

subscriber to have their own. The maximums may all be the same or they may not thus allowing preferential treatment to select subscribers. The "profile" is used to differentiate one subscriber from another. Since Lin fails to consider GETS, POSTS, or connected subscribers, the reference can not be said to anticipate the current claims. Further, without Lin the other cited references fail to render the current claims obvious.

Examiner's response:

First of all, in HTTP, the Web browser establishes a connection to a Web server and sends an HTTP request message to the server. In response to an HTTP request message, performs any requested action, and returns an HTTP response message containing an HTML document in accord with the requested action, or an error message. The returned HTML document may simply be a file stored on the Web server, or may be created dynamically using a script called in response to the HTTP request message. For instance, to retrieve a document, a Web browser may send an HTTP request message to the indicated Web server, requesting a document by reference to the URL of the document. The Web server then retrieves the document and returns it in an HTTP response message to the Web browser. Request messages in HTTP contain a "method name" indicating the type of action to be performed by the server, a URL indicating a target object (either document or script) on the Web server, and other control information. The request methods defined in the current version of the HTTP protocol include GET, POST, PUT, HEAD, DELETE, LINK, and UNLINK. HEAD, DELETE, LINK and UNLINK are less commonly used. The GET method causes the server to retrieve the object indicated by the given URL and send it back to the client. If

the URL refers to a document, then the server responds by sending back the document. If the URL refers to an executable script, then the server executes the script and returns the data produced by the execution of the script. Web browser programs normally use the GET method to send request messages to the Web server to retrieve HTML documents, which the Web browser then displays on the screen at the client computer. The POST method sends data, usually the user input parameters from an HTML form, to the server. The POST request also contains the URL of a script to be run on the server. The server runs the script, passing the parameters given in the request, and the script generates an HTML output that is returned in the response to the client. In order for a client program to send arbitrary data to the Web server using the current HTTP protocol, the client program must use either the PUT method or the POST method, as these are the only two methods that allow such data transfer to the Web server. Web browsers generally use only the POST method and generally only for the purpose of sending data in connection with forms to be processed. That is why it is called session establishment requests as taught by the reference Lin.

Lin is effervescent in elucidating that "receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network. said request including a Universal Resource Locator (URL)", in col. 2, line 10-25, "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total

number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target. A source could be a single host, a group of hosts in a network or domain, or any number of hosts in the entire Internet. By the same token, a target could involve one or more hosts and servers in an internal network. However, the most likely scenario of a DoS attack occurs from an arbitrary host in the Internet to a specific site in an internal network. This specific site is usually represented by a single domain name or a virtual IP (VIP) address."

Lin thereby teaches that Dos includes the existing sessions to a specific site in an internal network represented by a single domain name or virtual IP (VIP) address.

Lin also teaches in col. 2, line 63-66, "By selectively passing some of the session establishment requests, the filter 106 allows at least some legitimate session requests to get through to the target 104 (unlike the prior art "total blocking" method). "

Lin thereby teaches that Dos includes the existing sessions to a specific site in an internal network represented by a single domain name or virtual IP (VIP) address wherein legitimate session request is determined. (The "profile" is used to differentiate one subscriber from another.)

Applicant's argument:

With regard to the Examiner's Note on page 13 of the Office Action, the Applicant respectfully counters that the Office is obligated to provide a complete prosecution history for appropriate review. If a rejection lacks sufficient logical or technical support, then the burden of the Applicant is met by merely pointing this out. The Applicant will

not endeavor to speculate on ways to reform the rejection. If the Applicant were to respond only to the Applicant's formulation of the rejection and not to the rejection as written, then they risk having their arguments deemed non-responsive.

Examiner's response:

The grounds of rejection are 35 USC § 102 and 35 USC § 103. Providing citations is merely pointing out the teachings of the prior art.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 2, 5, 13, 16, 24 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Lin et al. (hereinafter Lin)(US 6,751, 668).

Referring to claim 2,

The reference teaches a method for preventing denial of service attacks (col.1, lines 7-10) against Hypertext Transfer Protocol (HTTP) servers (col.2, lines 17-25) the method comprising:

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network. said request including a Universal Resource Locator (URL), (col.2, lines 21-25)

receiving a profile for said subscriber; filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, (col.2, lines 63-66, col.4, lines 14-18) said filtering including:

updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency

and forwarding said request to said at least one other communication network when said subscriber is authorized to make said request. (col.2, lines 26-62, col.4, lines 14-18).

Referring to claim 5,

The reference teaches the method wherein said applying further comprises dropping the data packet containing said request when said client HTTP request frequency exceeds said maximum HTTP request frequency. (col.2, lines 33-39, lines 63-66).

Referring to claim 13,

Claim 13 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 2. Therefore, claim 13 is rejected for the reasons set forth for the claim 2.

Referring to claim 16,

Claim 16 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 5. Therefore, claim 16 is rejected for the reasons set forth for the claim 5.

Referring to claim 24,

Claim 24 is a claim to an apparatus carrying out the method of claim 2. Therefore, claim 24 is rejected for the reasons set forth for the claim 2.

Referring to claim 27,

Claim 27 is a claim to an apparatus carrying out the method of claim 5. Therefore, claim 27 is rejected for the reasons set forth for the claim 5.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3, 4, 6, 14, 15, 17-20, 25, 26 and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al. (hereinafter Lin)(US 6,751, 668) in view of Primeaux et al. (hereinafter Primeaux) (US 6,334,121).

Referring to claims 3 and 4,

Keeping in mind the teachings of the reference Lin as stated above, the reference fails to teach setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency and sending said alarm to an Internet Service Provider (ISP) associated with subscriber. The reference Primeaux teaches the action taken could be defined to suspend the user account or merely mail a message to the system administrator (sending alarm to an Internet Service Provider (ISP) associated with subscriber), warning of a potential intruder including the category of users such as

Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (dropping the data packet containing request). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin's capabilities with Primeaux's usage pattern tracking capabilities and applying the attack preventive measures based on the set threshold levels such as client HTTP request frequency exceeding a maximum HTTP request frequency and setting an alarm to the ISP (the system administrator).

Referring to claims 6, 7, 8 and 9,

Keeping in mind the teachings of Lin as stated above, although the reference teaches disabling HTTP requests for a hold-down period when said client HTTP request frequency exceeds said maximum HTTP request frequency. (Fig. 4, "shaded area"), the reference fails to teach shutting down the account used to access first communication network when said client HTTP request frequency exceeds said maximum HTTP request frequency and increasing said hold-down period each time said client HTTP request frequency exceeds said maximum HTTP request frequency, and wherein said hold-down period increases exponentially each time said client HTTP request frequency

exceeds said maximum HTTP request frequency. The reference Primeaux teaches the action taken could be defined to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) or merely mail a message to the system administrator, warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (hold-down period each time client HTTP request frequency exceeds said maximum HTTP request frequency and hold-down period increases exponentially each time client HTTP request frequency exceeds maximum HTTP request frequency). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as client HTTP request frequency exceeding a maximum HTTP request frequency set by the security rules and to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) as desired, based on the level of security

awareness that the software is set for (hold-down period each time client HTTP request frequency exceeds said maximum HTTP request frequency and hold-down period increases exponentially each time HTTP frequency exceeds maximum HTTP request frequency) when client HTTP request frequency exceeds a maximum HTTP frequency. This provides a system wherein the system will detect a difference in the pattern of usage. When such a difference is detected, the system will take the appropriate action.

Referring to claims 14 and 15,

Claims 14 and 15 are claims to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claims 3 and 4. Therefore, claims 14 and 15 are rejected for the reasons set forth for the claims 3 and 4.

Referring to claims 17, 18, 19 and 20,

Claims 17, 18, 19 and 20 are claims to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claims 6, 7, 8 and 9. Therefore, claims 17, 18, 19 and 20 are rejected for the reasons set forth for the claims 6, 7, 8 and 9.

Referring to claims 25 and 26,

Claims 25 and 26 are claims to an apparatus carrying out the method of claims 3 and 4. Therefore, claims 25 and 26 are rejected for the reasons set forth for the claims 3 and 4.

Referring to claims 28, 29, 30 and 31,

Claims 28, 29, 30 and 31 are claims to an apparatus carrying out the method of claims 6, 7, 8 and 9. Therefore, claims 28, 29, 30 and 31 are rejected for the reasons set forth for the claims 6, 7, 8 and 9.

8. Claims 36-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al. (hereinafter Lin)(US 6,751, 668) in view of Primeaux et al. (hereinafter Primeaux) (US 6,334,121). as applied to claims above, and further in view of Prabandham et al. (hereinafter Prabandham)(US 6,701,438).

Referring to claim 36,

The reference Lin teaches a first receiving interface capable of accepting a HTTP request received from a subscriber using a first communication network., said request including a Universal Resource Locator (URL);(Fig. 1, element 106); a profile request generator capable of generating a profile request based upon said request; (col.2, lines 63-66); a filter capable of determining whether said request is authorized based upon said requested profile. said filter including; an updater to update a client HTTP request count when said request for said URL is a HTTP "GET" request or a HTTP "POST" request', and

a responder to apply HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency; (col.2, lines 26-66, col.4, lines 14-18). Keeping in mind the teachings of the references Lin and Primeaux, both of these references fails to a first forwarding interface capable of sending said profile request to an Authentication, Authorization, and Accounting (AAA) server; a second receiving interface capable of

accepting a requested profile; an authorizer capable of allowing said request to be forwarding on at least one other communication network coupled to said first communication network: and a second forwarding interface capable of forwarding said request on said at least one other communication network. The reference Prabandham teaches an authorizer capable of allowing said request said request to be forwarded on at least one other communication network coupled to said first communication network. (Fig. 2, element 216 and col.4, line 67 and col. 5, lines 1-8); a first forwarding interface capable of sending said profile request to an AAA server; (element 212 which has the first receiving interface which is AAA server); a second receiving inter-face capable of accepting a requested profile; and a second forwarding interface capable of forwarding said request on said at least one other communication network. (element 216's interfaces connected to element 212 and element 206). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin with Primeaux's usage pattern tracking capabilities and Prabandham's security protocols. In this way, it will provide an alternative to the Lin's system for an user AAA verification, in addition to filter's capability to selectively passing some of the session establishment requests.

Referring to claims 37 and 38,

Claims 37 and 38 are rejected for the reasons set forth for the claims 3 and 4.

Referring to claim 39,

The reference Lin teaches the method wherein the responder drops the data packet containing said request when said client HTTO request frequency exceeds said maximum HTTP request frequency. (col.2, lines 33-39, lines 63-66).

Referring to claims 40, 41, 42 and 43,

Claims 40, 41, 42 and 43 are rejected for the reasons set forth for the claims 6,7,8 and 9.

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on (571) 272-3964. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100